ATTACHMENT - CLAIMS LISTING

This listing of claims will replace all prior versions, and listings, of claims in the application.

1. (Canceled)

2. (Previously Presented) A method according to claim 130, in which the predetermined authentication information stored by each authentication storage device corresponds to information which is used to authenticate a user of that authentication storage device in relation to the telecommunications system.

3. - 4. (Cancelled)

5. (Currently Amended) A method according to claim 130, wherein said authenticating step includes authenticating each user ~~is authenticated~~ in the telecommunications system by use of a smart card or subscriber identity module, and in which the storing step of the at least one authentication storage device includes predetermined authentication information respective to that user which corresponds to or simulates the smart card for that user.

6. (Previously Presented) A method according to claim 5, wherein the smart card or subscriber identity module authenticates the transaction after the smart card or subscriber identity module is operable in a terminal usable in a mobile and/or cellular telecommunications system.

7. (Currently Amended) A method according to claim 6, wherein the smart card or subscriber identity module ~~is operable to~~ authenticates the terminal in the mobile and/or cellular telecommunications system.

8. - 10. (Cancelled)

11. (Currently Amended) A method according to claim 130, further including the step of incorporating ~~in which~~ the authentication storage device ~~is incorporated~~ on a data carrier for data or software for use by that data processing apparatus.

12. (Previously Presented) A method according to claim 130, in which the authenticating step includes the steps of sending of a message, and generating a response dependent on the message and the predetermined information.

13. - 16. (Cancelled)

17. (Previously Presented) A method according to claim 130, further including the step of operatively coupling the authentication storage device for communication over a carrier with the transaction manager.

18. (Cancelled)

19. (Previously Presented) A method according to claim 17, wherein the carrier is operatively coupled to the data processing apparatus by a wireless link.

20. (Previously Presented) A method according to claim 17, wherein the authentication storage device is removably coupled to the carrier.

21. (Cancelled)

22. (Previously Presented) A method according to claim 17, comprising the step of using said carrier to obtain user security data independently of the data processing apparatus, and analysing the user security data for determining whether to allow access to the predetermined information.

23. (Original) A method according to claim 22, wherein the security data is obtained by alphanumeric data entry.

24. (Cancelled)

25. (Previously Presented) A method according to claim 22, wherein the user security data comprises a Personal Identification Number (PIN) and the analysing step compares the PIN obtained by the security data entry device with a PIN stored on the authentication storage device and only allows access to the predetermined information when the respective PINs match.

26. (Cancelled)

27. (Previously Presented) A method according to claim 17, wherein communication with the data processing apparatus is controlled by a data processing module.

28. - 29. (Cancelled)

30. (Previously Presented) A method according to claim 27, wherein the data processing module of the carrier decrypts encrypted data received from the data processing module of the data processing apparatus.

31. (Previously Presented) A method according to claim 27, wherein the data processing module of the carrier encrypts data transmitted to the data processing module of the data processing apparatus.

32. (Previously Presented) A method according to claim 30, wherein the respective data processing modules comprise a key for allowing encryption and/or decryption of data.

33. (Previously Presented) A method according to claim 32, wherein the key comprises a shared secret key for each of the respective data processing modules.

34. (Previously Presented) A method according to claim 17, wherein the carrier is operatively coupled to a plurality of authentication storage device for respectively enabling the said authentication process and one or more other authentication processes.

35. (Cancelled)

36. (Previously Presented) A method according to claim 130, including routing communications between the authentication storage device and the telecommunications system via the transaction manager.

37. (Previously Presented) A method according to claim 130, wherein the transaction manager is implemented by the data processing apparatus.

38. (Previously Presented) A method according to claim 130, wherein the transaction manager detects the operative coupling of the authentication storage device.

39. (Previously Presented) A method according to claim 36, wherein the transaction manager transmits data relating to an authenticated transaction to the entity to which that transaction relates.

40. - 51. (Cancelled)

52. (Currently Amended) Data processing system for carrying out an authentication process for authenticating a transaction by any one of a plurality of users with an entity, said data processing system comprising:

a data processing apparatus,

a selected one of a plurality of authentication storage devices in operative association with the data processing apparatus, each said authentication storage device storing predetermined authentication information relating to the carrying out of the authentication process, the entity being operable to generate transaction data relating to the transaction, and

a common telecommunications system which is registerable with the plurality of the authentication storage devices,

a communications link with the telecommunications system by which each of the authentication storage devices is operatively associated with the data processing apparatus to carry out the authentication process, and

an authenticating device incorporated in the telecommunications system by which the authentication process is carried out and which involves the use of the predetermined authentication information respective to the user stored by the selected one authentication storage device~~s~~, the predetermined authentication information being stored by each authentication storage device~~s~~ corresponding to information which is used to authenticate a telecommunications terminal of that user in relation to the telecommunications system but the authentication process for authenticating the transaction by that user with the data processing apparatus not requiring use of that user's telecommunications terminal,

the data processing apparatus comprising at least a transaction manager through which communications between the data processing apparatus and the telecommunications system are transmitted and through which the predetermined authentication information is also transmitted between the authentication storage device and the telecommunications system, the transaction manager being implemented by the data processing apparatus.

53. (Previously Presented) A data processing system according to claim 52, in which the predetermined authentication information stored by each authentication storage device corresponds to information which is used to authenticate a user of that authentications storage device in relation to the system.

54. - 55. (Cancelled)

56. (Previously Presented) A data processing system according to claim 53, in which each user is authenticated in the telecommunications system by the use of a smart card or subscriber identity module, and in which the authentication storage device respective to that user corresponds to or simulates the smart card for that user.

57. (Previously Presented) A data processing system according to claim 56, wherein the smartcard or subscriber identity module is operable in a terminal usable in a mobile and/or cellular telecommunication system to authenticate the transaction.

58. (Previously Presented) A data processing system according to claim 57, wherein the smartcard or subscriber identity module is operable to authenticate the terminal in the mobile and/or cellular telecommunication system.

59.- 60. (Cancelled)

61. (Previously Presented) A data processing system according to claim 52, in which the authentication process involves the sending of a message and the generation of a response dependent on the message and the predetermined information.

62. – 65. (Cancelled)

66. (Previously Presented) A data processing system according to claim 52, wherein a carrier is provided for the authentication storage device and the authentication storage device is operatively couplable to the carrier.

67. (Cancelled)

68. (Previously Presented) A data processing system according to claim 66, including a communication device for wireless communication between the carrier and the data processing apparatus.

69. (Previously Presented) A data processing system according to claim 66, including a coupling device removably coupling the carrier to the authentication storage device.

70. (Cancelled)

71. (Previously Presented) A data processing system according to claim 66, wherein the carrier includes means for obtaining user security data independently of the data processing apparatus and means for analysing the user security data for determining whether to allow access to the predetermined information.

72. (Previously Presented) A data processing system according to claim 71, wherein the carrier comprises an alphanumeric data entry device allowing the security data to be obtained.

73. (Cancelled)

74. (Previously Presented) A data processing system according to claim 71, wherein the user security data comprises a personal identification number (PIN) and the analysing device is operable to compare the PIN obtained by the security data entry device with a PIN stored on the authentication storage device and for only allowing access to the predetermined information when the respective PINs match.

75. (Cancelled)

76. (Previously Presented) A data processing system according to claim 66, wherein the carrier comprises a data processing module for controlling communication with the data processing apparatus.

77. - 78. (Cancelled)

79. (Previously Presented) A data processing system according to claim 76, wherein the data processing module of the carrier includes a decrypting device decrypting encrypted data received from the data processing module of the data processing apparatus.

80. (Previously Presented) A data processing system according to claim 76, wherein the data processing module of the carrier encrypts data transmitted to the data processing module of the data processing apparatus.

81. (Previously Presented) A data processing system according to claim 79, wherein the respective data processing modules comprise a key for allowing encryption and/or decryption of data.

82. (Previously Presented) A data processing system according to claim 81, wherein the key comprises a shared secret key for each of the respective data processing modules.

83. (Previously Presented) A data processing system according to claim 66, wherein the carrier includes a coupling device operatively coupling the carrier to a plurality of authentication storage device for respectively enabling said authentication process and one or more other authentication processes to be performed.

84. (Cancelled)

85. (Previously Presented) A data processing system according to claim 52, wherein data communications between the authentication storage device and the telecommunications system are routed via the transaction manager.

86. (Previously Presented) A data processing system according to claim 52, wherein the transaction manager is implemented by the data processing apparatus.

87. (Previously Presented) A data processing system according to claim 52, wherein the transaction manager is operable to detect the operative coupling of the authentication storage device to the data processing device.

88. (Previously Presented) A data processing system according to claim 52, wherein the transaction manager is operable to transmit data relating to an authenticated transaction to the entity to which that transaction relates.

89. - 129. (Cancelled)

130. (Currently Amended) A method for carrying out an authentication process for authenticating a transaction by one of a plurality of users with an entity, said method comprising the steps of:

storing, on at least one authentication storage device of an authenticator of a telecommunications system, selected ones of a plurality of respective predetermined authentication information of each respective ones of the plurality of users, the respective predetermined authentication information corresponding to an actual authenticating information of a mechanism provided in a telecommunications terminal of each respective user which telecommunications terminal is associated with the telecommunications system;

initiating by one user a desired transaction with the entity, said initiating step including the steps of establishing a communication between a transaction manager of the one user and a data processing apparatus of the entity and

supplying of data by the user to the data processing apparatus of the entity;

generating, by the data processing apparatus of the entity using the supplied data, transaction data relating to the desired transaction of the one user;

authenticating the one user to the data processing apparatus of the entity before completing the transaction, said authenticating step including the steps of

establishing a connection, via a common telecommunications system, between the data processing apparatus of the entity and the authentication storage device of the authenticator having the predetermined authentication information of the one user,

implementing the transaction manager of the user by the data processing apparatus of the entity, said implementing step including the step of

transmitting the transaction data between the data processing apparatus of the entity and the telecommunications system, and

transmitting the actual authenticating information of the telecommunications terminal of the user to the authenticator, said transmitting step not requiring use of the telecommunications terminal of the user;

comparing the predetermined authentication information of the authentication storage device with the actual authenticating information by the authenticator to determine ~~if~~ whether there is a match, and where there is a match communicating ~~a~~ the match to the transaction manager; and

completing the desired transaction of the one user by the data processing apparatus if a match is communicated to the transaction manager.